IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Luz Maria Camacho et al.	Confirmation No. 4973
Serial No.: 09/801,468	Examiner: Brown, Christopher J. Art Unit: 2134
Filed: March 7, 2001	Atty. Docket No. 010942-0269936 AWT-003
For: Method and Apparatus for Reducing On-Line Fraud Using Personal Digital Identification	

Submitted electronically via EFS

REPLY BRIEF

Mail Stop APPEAL
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This paper is further to the Examiner's Answer mailed August 8, 2006, for which a reply brief is due October 8, 2006. Applicant claims small entity status, see 37 CFR 1.27. A Request for Oral Hearing is being submitted concurrently with this brief. The Commissioner is authorized to charge the $500.00 for the Request for Oral Hearing and any other required fee to Pillsbury Winthrop Shaw Pittman LLP's deposit account no. 03-3975 (order no. 010942-0269936).

THE EXAMINER IGNORES CLEAR CLAIM LIMITATIONS AND DISREGARDS THE INVENTION AS A WHOLE

In evaluating claims, all claim limitations must be considered and given weight. MPEP 2143.03. Moreover, it is improper to distill an invention down to a hypothetical "gist" or "thrust" of the invention. Rather, the invention as a whole must be considered. MPEP 2141.02. Simply put, the rules do not allow an Examiner to just pick and choose words from prior art references and rearrange those words to conform with the claim language.

Here, the claims require many elements, which taken as a whole, clearly provide many patentable distinctions over the cited prior art. For example, claim 1 requires:

> storing business rules for a plurality of companies having on-line resources;
>
> receiving a message indicating a request from a user to use on-line resources;
>
> identifying a company associated with the requested on-line resource from among the plurality of companies;
>
> retrieving the stored business rules for the identified company;
>
> determining whether the request requires authentication;
>
> enabling the request to be fulfilled without authentication if the determination indicates that authentication is not required;
>
> obtaining an indicia of physical identification from the user if the determination instead indicates that authentication is required;
>
> comparing the obtained indicia to a stored indicia for the user; and
>
> enabling the request to be fulfilled if the obtained indicia matches the stored indicia,
>
> wherein the step of determining whether the request requires authentication includes determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required.

Taken as a whole, this claim clearly defines a method of authenticating individual requests for use of on-line resources. The determination of whether authentication is required is based on stored business rules of a plurality of companies. The method requires identifying a company associated with the requested on-line resource, and retrieving that company's stored business rules. The determination includes determining whether the identified company's

retrieved business rules indicate that the particular user making the request for the particular requested on-line resource requires authentication.

Pereira merely shows a system that allows access to database objects by users who can be associated with a plurality of companies.

Viavant merely shows a system that determines when and how authentication of a client accessing a server is required.

Applicants respectfully submit that the claimed invention as a whole clearly defines over this alleged combination of references. Applicants further submit that there is a significant amount of subject matter in the claims that is not being given proper weight. While the Examiner is permitted to interpret claims broadly, the Examiner is not permitted to disregard claim limitations because they are considered obvious addition of words to other words. Rather, the Examiner must consider the limitations first, then consider whether the limitations are obvious in view of the cited references.

For example, claim 1 clearly defines a series of steps as follows:

> storing business rules for a plurality of companies having on-line resources;
>
> receiving a message indicating a request from a user to use on-line resources;
>
> identifying a company associated with the requested on-line resource from among the plurality of companies;
>
> retrieving the stored business rules for the identified company;

This claim requires three discrete steps of storing, identifying and retrieving particular types of information associated with a plurality of companies and requested on-line resources.

In rejecting this claim, the Examiner states that Pereira "teaches storing business rules for a plurality of users of different companies . . . , receiving a message from a user requesting access to online resources . . . , retrieving the rules according to the user . . . [and] identifying the company associated with online resources." (Answer at 4.) Here, the Examiner has changed the wording of the claim in many ways, thereby ignoring the invention as a whole. This allows the Examiner to stretch Pereira's teachings to cover a "gist" of the claimed invention.

Likewise, in the Answer, the Examiner states that:

> Pereira III teaches controlling access per company. . . . Pereira III teaches storing rules controlling access to a specific group of objects. In this instance, the database has the attribute of 'company' and in the example provided, gives user 3 conditional Read-Only access to Company A objects. Figure 3 [sic, should be Figure 2], shows object access control data, where each object is given a 'company' property, so that data objects may be restricted based on said company and user. Therefore the access control rules (business rules) are stored associating a company with a requested online resource from among a plurality of companies (companies A, B, or C). When the data object is requested, the access rules (business rules) are retrieved to determine whether the requester should be granted access. While Pereira III does teach that the rules are applied to users, they are also the rules for the companies involved.

This further demonstrates how the claim language has been twisted into a "gist" so as to conform them with Pereira. For example, the Examiner states that "the access control rules (business rules) are stored associating a company with a requested online resource from among a plurality of companies."

However, the claims require, inter alia, (1) storing rules for a plurality of companies having on-line resources, (2) identifying a company associated with a requested resource, and (3) retrieving rules for the identified company. These three steps are simply not performed by Pereira's system at all. Rather, the Examiner's position implies that these all happen when a data object is requested by a user.

At best, Pereira stores company information associated with a user, identifies a company associated with a user who is requesting an object, then retrieves access rules for that user. The clear and distinct limitations of the claims are not met just because the user's company is associated with the user.

Moreover, it is respectfully submitted that the final clear limitation of claim 1, "wherein the step of determining whether the request requires authentication includes determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required" is not met at all by the combination of references.

The Examiner's position is that Pereira teaches granting access to an object with rules that identify a company, and that Viavant teaches authentication. However, this final limitation

requires substantial subject matter that is missing from that combination. This claim as a whole requires storing business rules that allow a company to determine how and when authentication is required for its on-line resources requested by users. Only by reducing the invention to a "gist" of allowing access to objects using authentication can the Examiner support this rejection.

THE EXAMINER MIS-READS PEREIRA

In addition to contorting the claim language in a manner that attempts to render them closer to the cited prior art, the Examiner mis-reads the cited prior art.

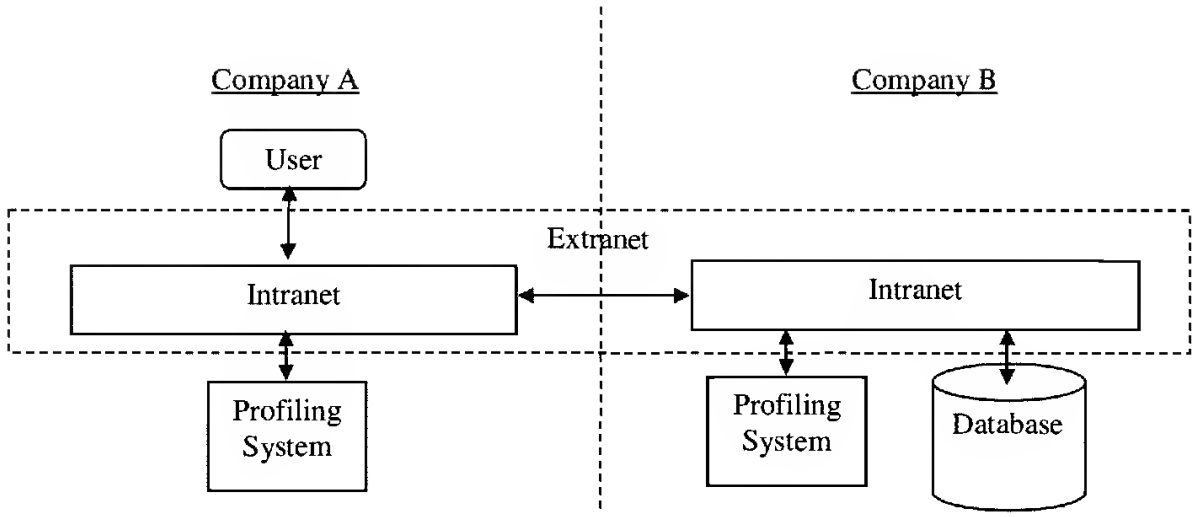
Pereira aims at "controlling access for a plurality of users to a plurality of objects located in at least one database." Col 2, lines 19-21. Each of Pereira's embodiments "may be used to control access to objects located in an electronic database on an Extranet." Col. 2, lines 50-52. According to Pereira, "in order to provide an Extranet user access to an object located in a foreign Intranet, the Intranet profiling system would need to include security data that gives the user access to the needed object. To reduce replication of profile records across Intranets, an Extranet profiling system may be used." Col. 3, lines 20-25. Pereira describes such an Extranet profiling system.

Fairly read, Pereira merely provides an access control system that allows users, who may belong to different companies, to access a single company's database via an Extranet. To avoid replication of information, Pereira teaches a Matrix access control database, wherein a "vertical component" (Figure 1 – containing user information) is linked to a "horizontal component" (Figure 2 – containing access information) based on a user ID.

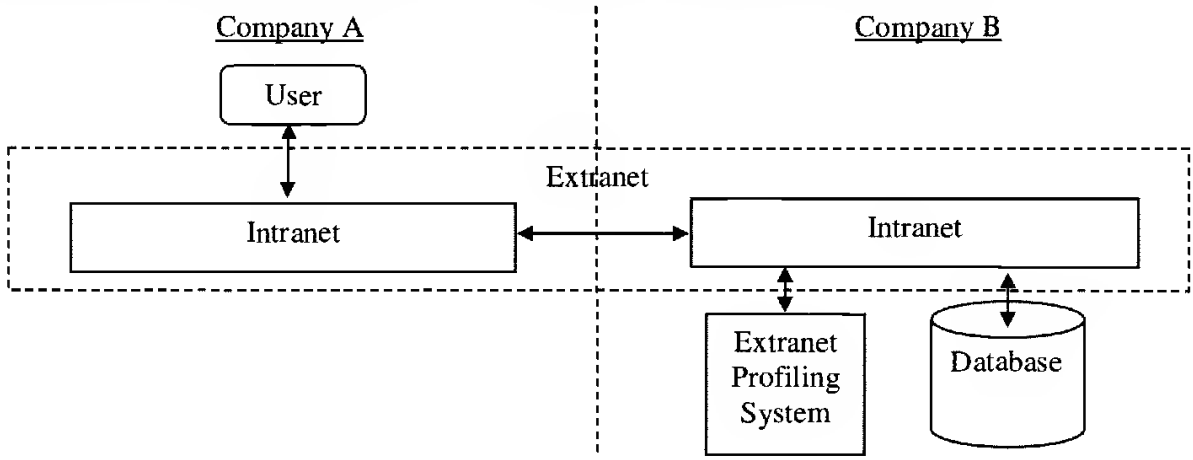
To repeat, Pereira merely teaches an access control system that allows access to a single company's database via an Extranet. Graphically, this is described below.

Although Pereira is somewhat unclear on details (any lack of clarity must be resolved in Applicants' favor), it appears that col. 2, lines 1-15 describe the problem as a user from Company A needing access to an object in Company B's database.

As shown below, according to Pereira, the problem is that the user's information is replicated among different profiling systems.



Pereira's "Extranet profiling system" solves this problem, which allows the User from Company A to access the database of Company B without requiring duplicate systems.



There is simply no teaching or suggestion in Pereira that this "Extranet profiling system" can provide access to more than one company's databases. Rather, it merely allows access to a single associated database from Extranet users without requiring individual "profiling systems" for each respective Intranet associated with different companies.

The Examiner states that Pereira's "database has the attribute of 'company' and in the example provided, gives user 3 conditional Read-Only access to Company A objects." This is unsupported and hypothetical. There is no statement in Pereira that the database contains "Company A objects." Pereira does disclose that access can be controlled for groups of objects in the same database. However, there is no suggestion that anyone other than the single

company whose database is made available to others via the Extranet can control access to objects in the database. At best, Pereira allows access to groups of objects in a database to be controlled for users based on a company they are associated with.

THE PRIOR ART DOES NOT SUGGEST HISTORICAL AUTHENTICATION PATTERNS

Dependent claims 2, 21 and 40 (as well as claims 46, 48 and 50 that depend therefrom) further require, *inter alia*, storing a profile of a user's authentication patterns with respect to a plurality of network elements, and determining a score based on the authentication patterns with the identified network elements.

The Examiner's Answer implicitly admits that the prior art does not disclose storing a user's historical authentication patterns. Rather than withdrawing the rejections, however, the Examiner's Answer states that "the term 'the user's historical authentication patterns' is not used before the claim argued. Without context and interpreted broadest reasonable interpretation, a historical authentication pattern could be interpreted as the pattern made up of the current call, or a plurality of communication attempts." (Answer at 9.)

Applicants respectfully submit that this position is in error. First, the Examiner's interpretation is broad but it is unreasonable. It completely writes the word "authentication" out of the claim. Authentication cannot be reasonably be interpreted as any type of attempt to make a call.

Moreover, claims 2, 21 and 40 depend from claims 1, 20 and 39 respectively. These claims set forth a context of authentication with respect to the invention. Accordingly, the Examiner's statement that the word authentication is not used before and does not have context is clearly incorrect.

For example, claim 1, from which claim 2 depends, requires, inter alia:

> determining whether the request requires authentication;
> enabling the request to be fulfilled without authentication if the determination indicates that authentication is not required;
> obtaining an indicia of physical identification from the user if the determination instead indicates that authentication is required;
> comparing the obtained indicia to a stored indicia for the user; and
> enabling the request to be fulfilled if the obtained indicia matches the stored indicia,

wherein the step of determining whether the request requires authentication includes determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required.

Clearly, the context of "historical authentication pattern" refers to the authentication that is conditionally performed in claim 1, which includes conditionally obtaining an indicia of physical identification from the user. Accordingly, claim 2 (as well as claims 21 and 40) have this authentication as context, and a historical pattern refers to a user's history of authentication as set forth in the independent claims.

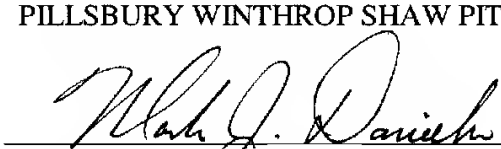
There is no suggestion in the prior art of storing a user's historical authentication patterns as clearly defined by the claims.

CONCLUSION

For the foregoing reasons, Appellants respectfully request that all the pending claims be deemed allowable by this honorable Board.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

Date: September 25, 2006



40,580
Reg. No.

Mark J. Danielson
Telephone: (650) 233-4777
Facsimile: (650) 233-4545
Please reply to customer no. 27,498